# D. Lgs n 231 e reati tributari

# Fattispecie di reati presupposto – art. 25 *quinquiesdecies*

| | |
|---|---|
| **Art. 2 c. 1** | Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti |
| **Art. 2 c. 2 *bis*** | Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti, nel caso in cui l'ammontare degli elementi passivi fittizi sia inferiore a 100.000,00 € |
| **Art. 3** | Dichiarazione fraudolenta mediante altri artifici |
| **Art. 4** | Dichiarazione infedele |
| **Art. 5** | Omessa dichiarazione |
| **Art. 8 c. 1** | Emissione di fatture o altri documenti per operazioni inesistenti |
| **Art. 8 c. 2 *bis*** | Emissione di fatture o altri documenti per operazioni inesistenti, nel caso in cui l'importo non rispondente al vero indicato nelle fatture o nei documenti, per periodo di imposta, sia inferiore a 100.000,00 € |
| **Art. 10** | Occultamento o distruzione di libri contabili |
| **Art. 10 *quater*** | Indebita compensazione |
| **Art. 11** | Sottrazione  fraudolenta al pagamento di imposte |

Nel 2019, la riforma dei reati tributari (**D.L. n. 124/2019**) ha esteso la **responsabilità 231 amplianto** i cosiddetti "**reati presupposto**", riducendo le soglie di punibilità e ampliando i livelli sanzionatori.

Alcuni reati tributari che rilevano ai fini della responsabilità dell'ente ex decreto 231 al contempo possono dare origine anche al delitto di autoriciclaggio

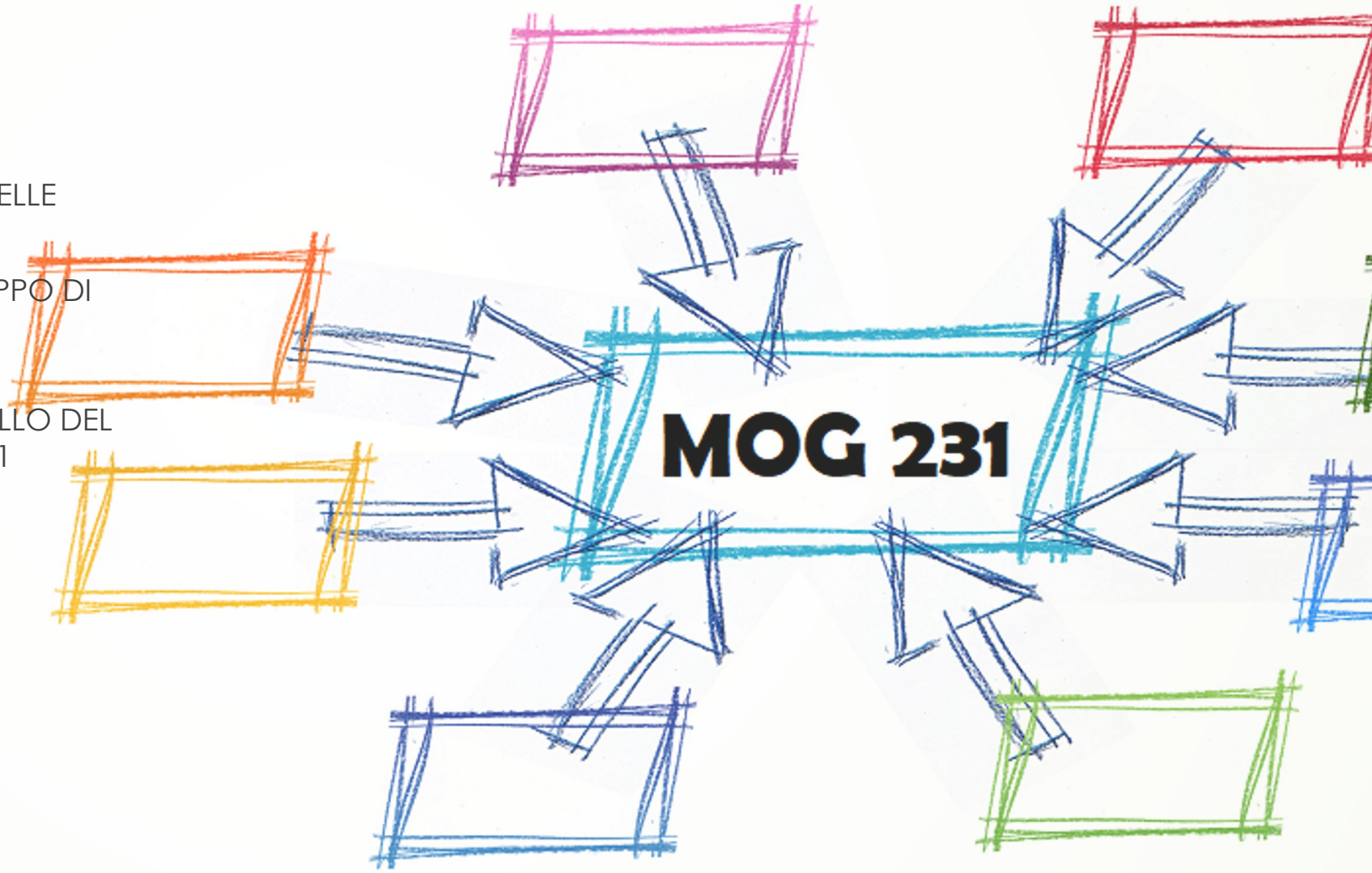
# Step organizzativi necessari

ANALISI STORIA FISCALE DELLA SOCIETA' E CONTROLLO DEI DOCUMENTI

MAPPATURA DEI PROCESSI E DELLE ATTIVITA' SENSIBILI

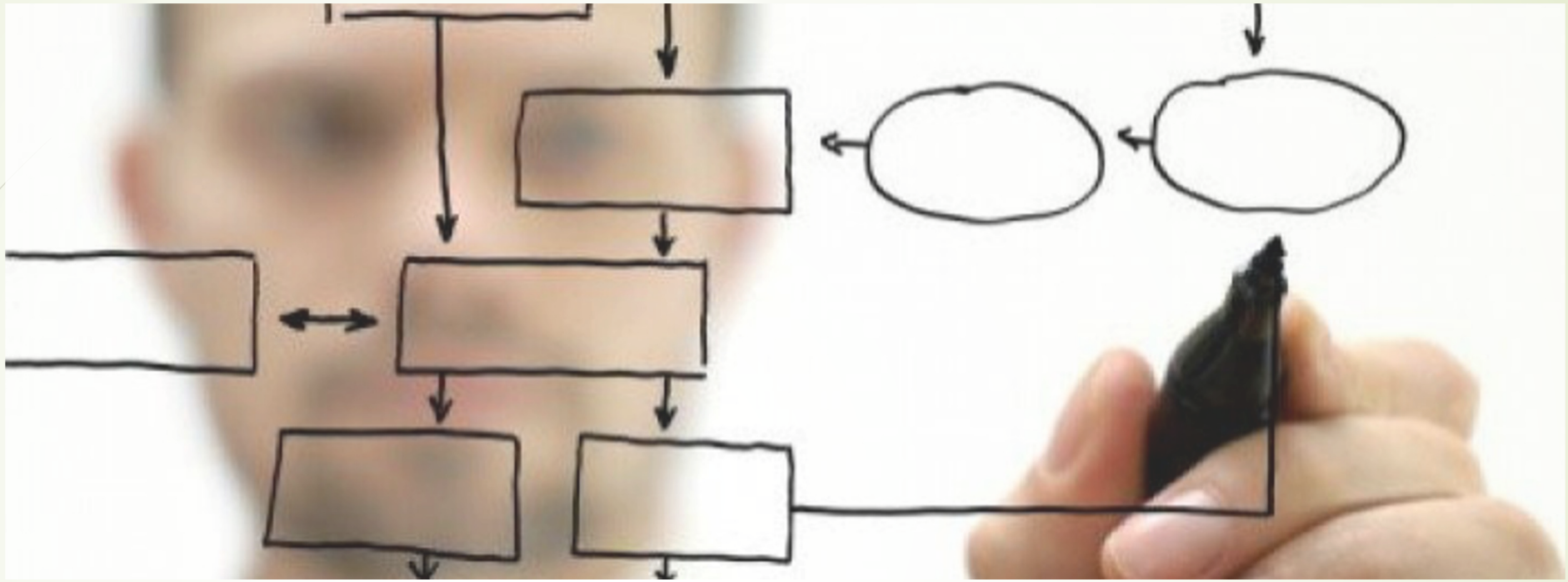
ANALISI, VALUTAZIONE E SVILUPPO DI UN ADEGUATO SISTEMA DI CONTROLLO INTERNO

AGGIORNAMENTO E CONTROLLO DEL MODELLO ORGANIZZATIVO 231



# D. Lgs n 231 e trattamento dei dati personali

Requisiti di Comformità e di Accountability del modello organizzativo Privacy



PREMESSA *I modelli organizzativi privacy, tenendo conto dei rischi emergenti dalle attività aziendali che richiedono il trattamento dei dati personali ex art. 4 n. 2) del Regolamento n.679/2016, risultano quindi utili, se non fondamentali, per garantire la prevenzione dell'eventuale responsabilità dell'azienda derivante da reati commessi in suo vantaggio e/o interesse da dipendenti o soggetti in posizioni apicali all'interno della stessa.*

**Il modello organizzativo privacy (anche MOP) ha la finalità primaria di dare evidenza delle azioni poste in atto da un'organizzazione per far fronte agli adempimenti in materia di protezione dei dati. In realtà tale documento potrebbe avere scopi ben più ampi.**

# GDPR e D. Lgs. 231/2001, punti di contatto e divergenze

## Art. 25 del GDPR

nel definire la *privacy by design* e by default (***protezione dei dati fin dalla progettazione del sistema e per impostazione predefinita***), fa riferimento all'adozione, da parte del titolare del trattamento, di "*misure tecniche e organizzative adeguate, in modo da attuare efficacemente i principi di protezione dei dati e da garantire nel trattamento i requisiti del Regolamento e la tutela dei diritti degli interessati*".

## Art. 6 comma 2 lett. b) del D. Lgs. 231/2001

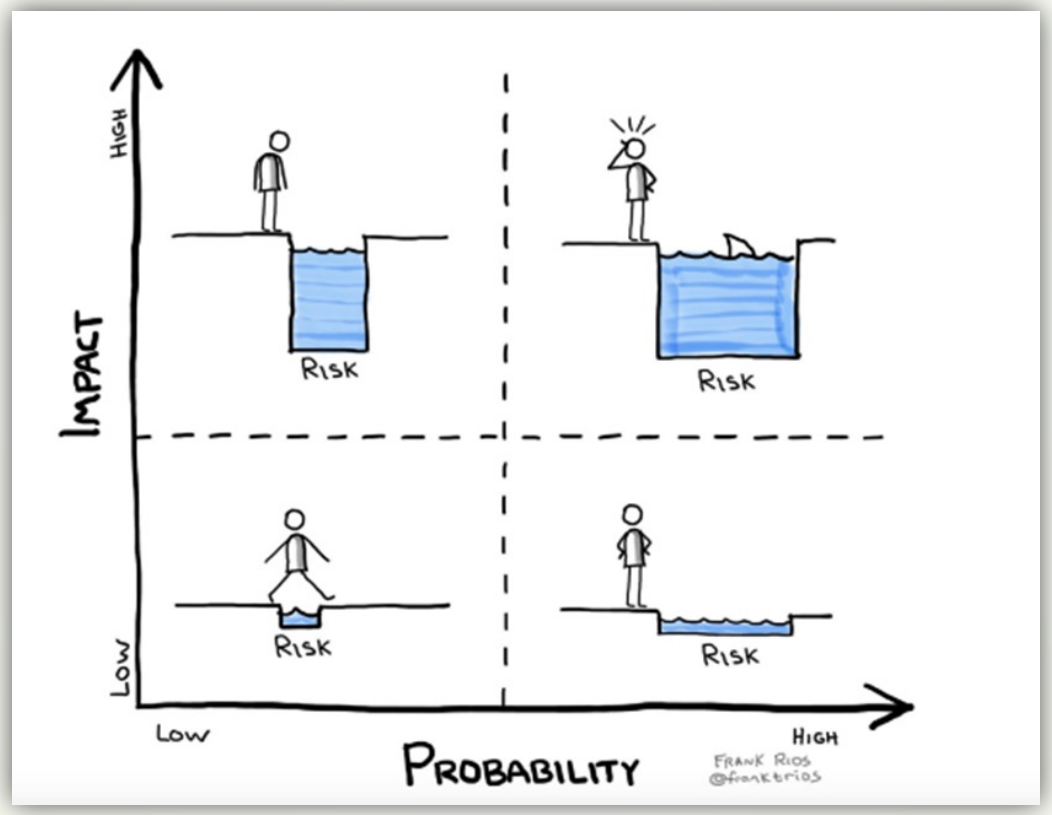
definisce i modelli di organizzazione e gestione dell'ente e stabilisce che questi devono "*prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*".

Entrambe le discipline convergono sulla necessità di prassi standardizzate al fine di garantire la conformità delle attività aziendali alle normative vigenti e vagliare i rischi sottesi a tali attività, c.d. ***risk-based approach*** prerequisito per individuare misure tecniche e organizzative adeguate

# Il modello organizzativo privacy è un sistema basato sulla valutazione del rischio

| COMFORMITA' | ACCOUNTABILITY |
|---|---|
| **Caratteristiche di conformità del modello organizzativo alle disposizioni del GDPR** | **Caratteristiche di un modello organizzativo tali che possano identificare il titolare del trattamento come "Accountable" secondo il GDPR** |
| Bisogna fare riferimento ai principi generali e alle disposizioni del Regolamento e del Codice di cui dobbiamo tenere conto nel costruire il nostro modello | Bisogna fare riferimento ad alcune «buone pratiche» per costruire un modello organizzativo privacy «robusto» che possa supportare il titolare nel raggiungimento del suo obiettivo di «accountability» |

# Definizione di rischio



Nel GDPR esistono comportamenti scorretti ed eventi informatici malevoli che possono integrare fattispecie di reato, le quali, se derivanti da condotte di soggetti interni all'azienda, possono costituire il presupposto per innescare la responsabilità dell'ente stesso.

| | |
|---|---|
| **INSIDERS** | comportamenti sleali e/o fraudolenti da parte dei dipendenti, che possono integrare il reato previsto e punito dall'art. 513 c.p delitto presupposto per configurare la responsabilità dell'impresa ex art. 25 bis.1 del D. Lgs. 231/2001 |
| **CYBERATTACK** | condotte di cyber sabotaggio che mirano a generare il malfunzionamento delle macchine, l'indisponibilità o degrado degli strumenti, ad accedere a sistemi telematici senza autorizzazione, a intercettare informazioni in rete |

# Delitti in materia di **privacy** contemplati dal D.lgs. 231/2001

i reati informatici D.lgs 231/2001 Art. 24-bis (delitti informatici e trattamento illecito di dati);

i reati in materia di copyright D.lgs 231/2001 Art. 25-novies ("delitti in materia di violazione del diritto d'autore") nel cui ambito rientrano i delitti c.d. di pirateria informatica.

Art. 24 *bis* del D.lgs. 231/2001_*Delitti informatici e trattamento illecito di dati*

I reati informatici commessi nell'interesse o vantaggio dell'ente da parte di soggetti apicali o preposti ne determinano la responsabilità amministrativa dell'ente stesso

Art. 4 Reg. Europeo

Questi sono tutte ipotesi di *data breach* dolosi o di violazioni informatiche

# Delitti informatici

| |
|---|
| accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) |
| intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (**art. 617-*quater* c.p.**) |
| installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (**art. 617-*quinquies* c.p.**) |
| danneggiamento di informazioni, dati e programmi informatici (**art. 635-*bis* c.p.**) |
| danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (**art. 635-*ter* c.p.**) |
| danneggiamento di sistemi informatici o telematici (**Art. 635 quater c.p.)** |
| danneggiamento di sistemi informatici o telematici di pubblica utilità (**Art. 635 quinquies c.p.)** |
| frode informatica del certificatore di firma elettronica (**Art. 640 quinquies c.p.)** |

# Esempi

| |
|---|
| Un dipendente compie un accesso abusivo d un sistema informatico di un'azienda concorrente al fine di acquisire informazioni sui clienti e sulle strategie commerciali **Art. 615-ter c.p.** |
| Un amministratore di sistema utilizza le password di accesso alle caselle e-mail dei dipendenti al fine di controllare le loro attività **Art. 615-quater c.p.** |

# Cybersecurity e gestione dei rischi

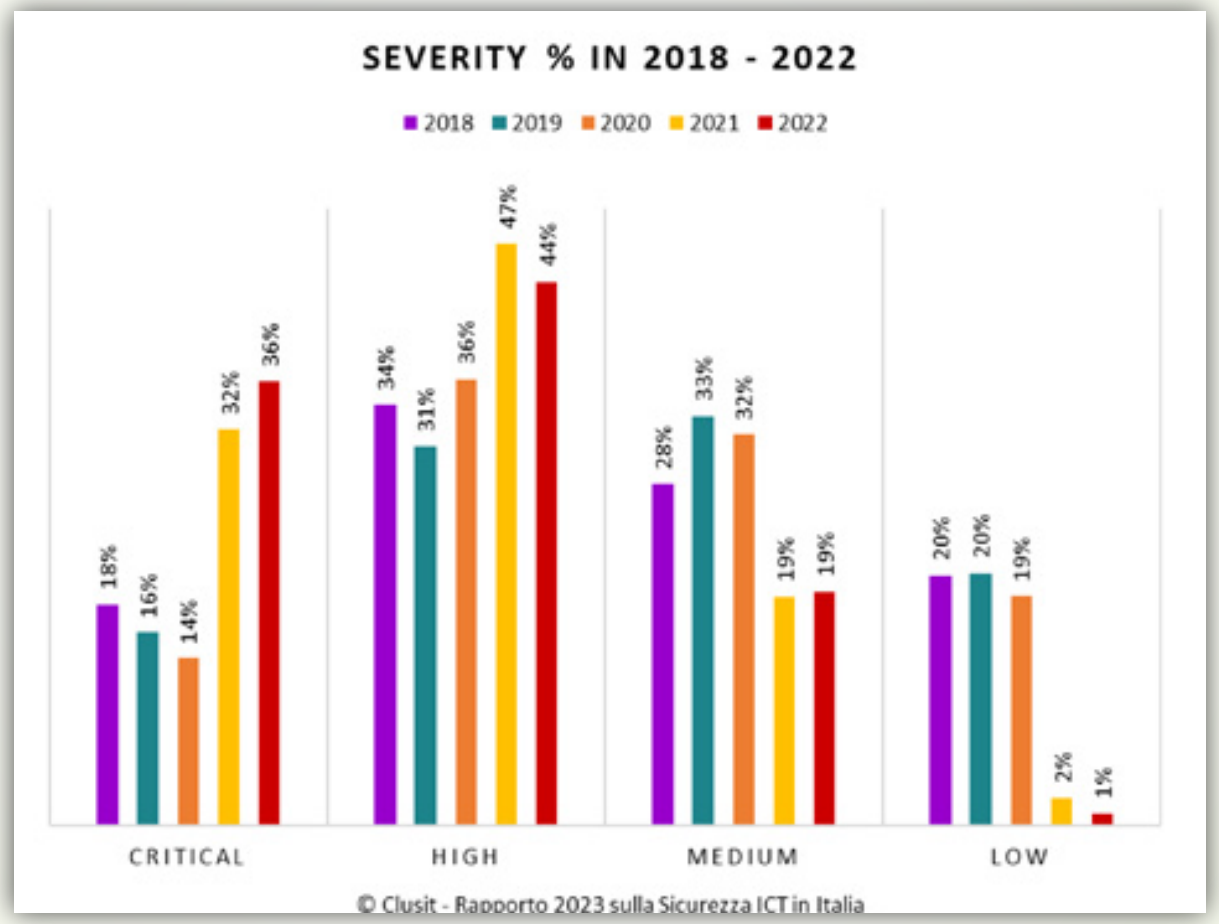
Nell'ambito dell'attività di predisposizione del Modello 231, la gestione dei rischi legati al mondo dell'informatica si fonda principalmente su tre pilastri:

**Prevenzione**

**Controlli**

**Formazione**

# Livello di gravità degli incidenti



# Crescita degli attacchi in Italia rispetto il resto del mondo

# Tecniche di attacco utilizzate